AFRL-IF-WP-TP-2002-501

INFORMATION ASSURANCE RELIABILITY MODEL (IARM)

Roberta L. Gotfried, Robert J. Moore, and Mark J. Kuckelman

SEPTEMBER 2002

Approved for public release; distribution is unlimited.

INFORMATION DIRECTORATE
AIR FORCE RESEARCH LABORATORY
AIR FORCE MATERIEL COMMAND
WRIGHT-PATTERSON AIR FORCE BASE, OH 45433-7334

NOTICE

When Government drawings, specifications, or other data are used for any purpose other than in connection with a definitely Government related procurement, the United States Government incurs no responsibility or any obligation whatsoever. The fact that the Government may have formulated or in any way supplied the said drawings, specifications, or other data, is not to be regarded by implication, or otherwise in any manner construed, as licensing the holder, or any other person or corporation; or as conveying any rights or permission to manufacture, use, or sell patented invention that may in any way be related thereto.

This report has been reviewed by the Office of Public Affairs (ASC/PA) and is releasable to the National Technical Information Service (NTIS). At NTIS, it will be available to the general public, including foreign nations.

This technical report has been reviewed and is approved for publication.

Tod J. Reinhart

TOD J. REINHART, Project Engineer
Embedded Information Systems Engineering Branch
AFRL/IFTA

James S. Williamson

JAMES S. WILLIAMSON, Chief
Embedded Information Systems Engineering Branch
AFRL/IFTA

James S. Williamson
For
Eugene C. Blackburn

EUGENE C. BLACKBURN, Chief
Information Technology Division
AFRL/IFT

IF YOUR ADDRESS HAS CHANGED, IF YOU WISH TO BE REMOVED FROM OUR MAILING LIST, OR IF THE ADDRESSEE IS NO LONGER EMPLOYED BY YOUR ORGANIZATION, PLEASE NOTIFY AFRL/IFTA, BLDG 620, 2241 AVIONICS CIRCLE, WRIGHT-PATTERSON AFB, OH 45433-7334 TO HELP US MAINTAIN A CURRENT MAILING LIST.

COPIES OF THIS REPORT SHOULD NOT BE RETURNED UNLESS RETURN IS REQUIRED BY SECURITY CONSIDERATIONS, CONTRACTUAL OBLIGATIONS, OR NOTICE ON A SPECIFIC DOCUMENT.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YY)* September 2002	**2. REPORT TYPE** Preprint	**3. DATES COVERED *(From - To)*** 04/10/2000 – 04/10/2002

4. TITLE AND SUBTITLE INFORMATION ASSURANCE RELIABILITY MODEL (IARM)	**5a. CONTRACT NUMBER** F33615-00-C-1628
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER 69199F
6. AUTHOR(S) Roberta L. Gotfried, Robert J. Moore, and Mark J. Kuckelman	**5d. PROJECT NUMBER** ARPI
	5e. TASK NUMBER FT
	5f. WORK UNIT NUMBER 0D
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Raytheon Electronics Systems Software Engineering Center 2000 E. Imperial Highway RE/R01/A521 El Segundo, CA 90245-3571	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Information Directorate Air Force Research Laboratory Air Force Materiel Command Wright-Patterson AFB, OH 45433-7334	**10. SPONSORING/MONITORING AGENCY ACRONYM(S)** AFRL/IFTA
	11. SPONSORING/MONITORING AGENCY REPORT NUMBER(S) AFRL-IF-WP-TP-2002-501

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

There are no current plans for publication of this material.

14. ABSTRACT

The objective of this effort is to design, develop, document, demonstrate, evaluate, and deliver science-based methods for information assurance (IA) design and assessment. The ultimate goal of the proposed research is to improve the IA reliability and robustness of systems overall and their ability to withstand asymmetric attacks. This shall be achieved by means of scientific methods and modeling techniques that assist in specifying requisite IA protection of a system, and in measuring the ability of a design or implementation of a system to meet that specification.

15. SUBJECT TERMS

information assurance, system security, information assurance modeling

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT:**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** (Monitor)
a. REPORT Unclassified	**b. ABSTRACT** Unclassified	**c. THIS PAGE** Unclassified	SAR	10	Tod J. Reinhart **19b. TELEPHONE NUMBER** *(Include Area Code)* (937) 255-6548 x3582

Abstract

This report summaries the work done under DARPA contract F33615-00-C-1628 by Raytheon Electronic Systems on the Information Assurance Reliability Model (IARM) during the calendar period of April 2000 to April 2001. The initial phase of our IARM work was performed under Michael Scroch as part of the Information Assurance Science and Engineering Tools (IASET) until November 2000 when a DARPA ITO re-organization transferred the IARM effort to the CyberPanel program under Catherine McCullough. Where the distinction is important, we will refer to the work done under these two DARPA programs as "phase 1" and "phase 2" respectively.

1 Introduction

The original motivation for the Information Assurance Reliability Model (IARM) program was the application of scientific and mathematical disciplines to advance the state of the art of the theory and practice of Information Assurance (IA). Initial disciplines to leverage as starting points were Reliability and Fault management. In the phase 1 conception of IARM, a method to provide a *static* evaluation of an information system was sought. The phase 1 model was found to have limitations when applied to real-time monitoring as desired under Cyber Panel in Phase 2. We attempted a more dynamic formulation in phase 2 driven by the needs of CyberPanel that appears to be more viable. However, we were not able to develop the dynamic formulation past a conceptual model in the reduced resources allotted for the program. In the phase 2 effort we also investigated other aspects of the model, such as human behavioral modeling, experimental validation, and real-time IA reliability monitoring which we recognized would be important components for IARM within Cyber Panel.

2 Mathematical Modeling (Phase 1)

Due to the complexity of IA systems, we decided that only stochastic models had a reasonable chance of success. After a brief period of research and evaluation, we decided to base our core IARM model on Markov chains. We documented our efforts in [1] where we proposed a conceptual IARM. We outlined the class of inputs needed for this model, and indicated how this model could be used to compute IA metrics. We proposed a baseline 7-state transition diagram (STD) to represent the IA characteristics of general IA systems to evaluate, including a detailed and rigorous definition of each state. The underlying model at this point was a discrete time Markov chain consisting of states with transition probabilities representing transitions between the states. We then performed a detailed analytic mathematical analysis of simplified two and three STDs and showed that the underlying discrete time Markov chain could be solved and had a meaningful interpretation in the context of IA as documented in [2]. We quickly determined that numerical solutions could be readily computed as illustrated in [3] for the baseline 7-state STD. The fact that probabilities were involved in the original model placed severe restrictions on proposed methods to compute the requisite transition probabilities. We documented the basic properties of such probabilities in [4]. We soon recognized that the use of DTMCs would make the actual determination of the transition probabilities very difficult if not impossible. We then performed a tradeoff between DTMCs and the corresponding continuous time Markov chains (CTMCs). We concluded that the latter we more appropriate to IARM. Happily CTMCs provided the solutions to several conceptual problems without being any more difficult to compute in practice. We proceeded to document an end-to-end example of all of the needed computations for a 7-state STD in [6] and provided the mathematical details in [7]. These examples were done using the basic Matlab (version 6) application. We also developed a simple GUI application to solve the 7-state STD in a more user-friendly manner and eliminated the need for Matlab. At this stage of the program we concluded that our basic approach was viable.

However, we recognized that very challenging practical problems remained. One major challenge would be the estimation of realistic transition rates from empirical data for actual IA systems. Even if the transition rate problem could be solved, we recognized the static nature of IARM limited its usefulness to those lifecycle phases when static analysis was adequate. Nonetheless, we felt that our initial approach advanced the state of the art in IA modeling for the original purposes of IARM and DARPA's IASET program. The objectives of Cyber panel in Phase 2 would require a radically different approach.

3. Figures of Merit and Metrics

The solution of a CTMC naturally provides several basic figures of merit such as the overall IA metric as well as metrics such as the estimated time until the system is compromised, or the expected time we expect a recovery will take as documented in [6] and [7].

4 Transition Rates (Phase 1)

In the development of IARM, we recognized that computing the STD transition probabilities (in the case of a DTMC) or transition rates (in the case of a CTMC) was a central, but difficult (and potentially intractable) problem. We first reasoned that there would be a dialectic between system defenses and system attackers. For example, stronger defenses against system penetration would necessarily reduce the probability of being penetrated. A stronger adversary would likewise increase the probability of being penetrated. For the original DTMC formulation of IARM, we attempted to derive expressions for the IARM transition probabilities (see for examples charts 8-10 of [3]. We concluded at the end of the phase 1 effort that such formulas were unrealistic in practice. This was one of the main reasons that the DTMC approach was abandoned in favor of a CTMC model since transition rates are not probabilities and not subject to the very strict requirements for probabilities [5]. In the case of a CTMC, we developed a method that in principle could be used to compute the needed CTMC transition rates [6] by observing the occupancy of the STD states at different points of time. However, redirection of the program in Phase 2 under Cyber Panel did not allow us to pursue experimentation to validate our analytical hypotheses.

In Phase 2 we performed a review of experiments that had been performed under Red Team efforts as part of Information Assurance & Survivability, to determine of any of the experiments had results that could be applied to validation of IARM. The results of this review were documented in [11]. It would be difficult to apply the results (or interim results) of many of the IA&S experiments to IARM due to a variety of reasons, which include

- Lack of measurements that could be turned into metrics and applied to a model;
- Complex objectives that make it difficult to determine how to apply the results of the experiments to a model;
- Lack of documented results.

The authors recommend that all future experiments incorporate some form of metrics collection or measurements in order to improve the chances of applicability and repeatability beyond the initial intent of the experiment and to better model information systems in the future.

5 Real Time Reliability Monitoring (Phase 2)

Under the Cyber Panel IARM Phase 2, we investigated the state-of-the-art as well as current research efforts in real-time reliability monitoring in an attempt to identify fruitful areas to pursue for Cyber Panel Big Board aspects.

Current research in this aspect of system reliability is receiving little research attention. We did identify one current effort in the area of monitoring nuclear reactors, where research is being performed both in the factors that need to be visible to the system operator, and the methods of display for human factors. These results were presented at the Cyber Panel PI meeting in April 2001[12]. Our conclusion is that in this area of real-time monitoring of system reliability, the field of Information Assurance has little to learn.

Our research proved much more fruitful when we looked at commercial and industrial application of these concepts. There is a growing market for real-time monitoring of systems that have high dependability requirements. Examples that were identified during the final phase of research include Internet Service Providers, heart monitors, manufacturing and assembly systems, and wireless and wide area networks. Both tools and service providers (e.g. *Reliamon*) are emerging. They are aided by growing experience in understanding symptoms that may indicate system failures at hardware and software levels. For example, Microsoft publishes guides and makes available tools for reliability monitoring. Representative references for these results can be found in [13].

Our conclusion is that similar approaches in IA reliability monitoring are very feasible. However, it will take considerably more experience in defending systems against IA attacks, and the gathering of quantitative as well as qualitative data with an intent to build a knowledge base from which useful tools and displays can be developed. It is our recommendation that experiments be designed with this specific objective in mind.

6 Top Level Architecture (Phase 2)

Before IARM was transferred from IASET to CyberPanel, we had already recognized the inadequacy of a static approach to IARM. Incorporation of IARM in CyberPanel would require a reformulation of several aspects of the overall IARM in order to address the dynamic real-time characteristics of the CyberPanel domain. The phase II top level architecture is documented in charts 5-10 of [8] where IARM is partitioned in three main modules: Markov, Transition Rates, and Human Behavior. A major difference in phase II is the adaptive formulation using real-time observations (and any other relevant data) from other components of CyberPanel. Thus transition rates are now short-term empirical data that reflect the current IA state of the system being monitored. The rates are now explicit functions of time. The problem of computing transition rate now appears more feasible in this context since we recognize that many other areas of engineering require such time dependent estimates. Once appropriate inputs are identified, obvious internal models of the transition rates might be based on a control theory state model (or perhaps Kalman filtering theory might be applicable). The transition rates then becomes parameters that are internally modeled and computed in an adaptive manner. Once estimates of the transition rates have been computed, the Markov module (which is identifiable with the CTMC model generated in Phase I) can be used to compute IA figures of merit as in Phase I.

The difference between Phases I and II is that the computed metrics in the latter are now short-term future predictions (instead of static predictions for all time, or at least as long as the system is not modified) which are updated each time one or more transition rates change value. An analogy is the Microsoft Windows estimate of the time required to complete a file download in progress, whose value is adjusted as network conditions vary.

7 Human Behavioral Modeling (Phase II)

The third phase II IARM module is the Human Behavior module. This is listed as a separate module since it captures an important aspect of IARM that is not covered by any other CyberPanel program. The basic approach for development of this module is given in [9].

It is clear that the IA behavior of a system is highly dependent on human behavior, including that of the attacker, the system administrator or security personnel, and users of the system. For example, a system with poor security personnel might be very vulnerable to attackers with poor skills. A highly capable attacker whose has a strong motive to harm your system may be hard to defend even with very capable security system administrators.

Several approaches to modeling human behavior were identified and leveraged the extensive work already done in such fields as sociology/criminology, psychology, and economics.

The modeling of human behavior in IA systems is highly dynamic and adaptive. The actions of the attacker and defender will be heavily dependent on the actions of the other. As such, our starting point for modeling human behavior was game theory. However, classical game theory was found to be inadequate for this purpose since it is too static. A search of the literature lead to other promising approaches based on elaborations of game theory such as algorithms based on self-adaptive genetic algorithm learning in game playing or stochastic games as just two candidates. A promising starting point would be to leverage work done where two simulated opponents play a game of simplified poker.

Significant work will be required to develop an adequate model of human behavior in IA systems. The first step was to study the extensive literature of the hacker culture and past system exploits and to develop a simplified attacker taxonomy. With the recent widespread use of the Internet, the nature of attacks on a computer system has profoundly changed. A good example is the ready availability of "click and point" attacker tools that unsophisticated attackers (often called "script kiddies") can use to successfully cause great damage to systems.

Thus, our initial work in modeling attacker behavior concentrated on identifying whether the attacker of a given system could be classified as a "script kiddie" or not. Because of the "canned" nature of attack tools, this seemed to be a good area for a proof of concept. Knowledge of whether or not the attacker of your system was a script kiddie or not would be a very valuable piece of information and would be a good starting point to demonstrate in an attacker model. If this was successful, further work would then concentrate on the "not a script kiddie" branch. Since insider attackers are estimated to be very prevalent, this might be the next type of attacker to model.

We again emphasize that the IARM human attacker model would be very adaptive and dynamic. For example, our estimate of the type of attacker would probably vary as a function of time, especially in the early stages of attack. Another area of research is how to validate such a model We have concluded that "red team" data would be of limited usefulness since for example both sides have too much information about each other. In addition, both sides lack important motivating elements. For example, the defender is not really worried about his system being destroyed while the attackers do not have to be concerned with being detected by law enforcement and possibly apprehended and prosecuted. However, some useful data does appear to be available in the form of "honeypot" projects and other instances in which attack behavior was observed and logged in great detail without the knowledge of the attacker.

Participants at the April 2002 PI meeting encouraged us to continue this area of research.

7 Conclusions

The results of IARM research during its two phases demonstrate that a reliability approach to Information Assurance of systems shows a lot of promise, and can contribute to more rapid maturation of the field and increased reliability of systems against IA attacks. The current predominance of IA research into defense against specific attacks, and the lack of useful metrics collection are ignoring this promising direction for research and system engineering.

The IARM researchers have observed that too little thought is being given to useful metrics to collect during system operation, and in the course of other IA research. For example, currently, it is common to measure the amount of time it takes a Red Team to attack a given system. However, metrics and observations related to the affect of various Red Team or hacker actions on a system would contribute significantly to the growth of IA reliability and the ability to integrate IA approaches within the system engineering process.

References

[1] R.J. Moore, *State Transition Diagram for the Information Assurance Reliability*, `iarm-std-wp.doc`, Unpublished Work of Raytheon Electronic Systems, May 2000)

[2] R.J. Moore, *Initial Mathematical Analysis of the IARM State Transition Diagram*, `iarm-mm-init-analysis.doc`, Unpublished Work of Raytheon Electronic Systems, June 2000

[3] R.J. Moore, *IARM Proof of Concept Vugraphs*, `iarm-poc-phase1.ppt`, Unpublished Work of Raytheon Electronic Systems, July 2000

[4] R.J. Moore, *Composition of Probabilities*, `iarm-mm-probability.doc`, Unpublished Work of Raytheon Electronic Systems, June 2000

[5] R.J. Moore, *IARM Math Models: Tradeoff of Discrete Time versus Continuous Time Markov Chains,* `iarm-dtmc-vs-ctmc.ppt`, Unpublished Work of Raytheon Electronic Systems, September 2000

[6] R.J. Moore, *IARM End-to-End Computational Example*, Systems, `iarm-end-to-end-example.ppt`, Unpublished Work of Raytheon Electronic Systems, November 2000

[7] R.J. Moore, *Fundamental Theory of the Information Assurance Reliability*, `iarm-theory.doc`, Unpublished Work of Raytheon Electronic Systems, December 2000)

[8] R.J. Moore, *IARM Proof of Concept Vugraphs, Phase II*, `iarm-poc-phase2.ppt`, Unpublished Work of Raytheon Electronic Systems, March 2001

[9] R.J. Moore, *Considerations in Modeling Human Behavior in Information Assurance*, `iarm-human-model.doc`, Unpublished Work of Raytheon Electronic Systems, March 2001

[10] R.J. Moore, *IARM Miscellaneous Vugraphs*, `iarm-misc.ppt`, Unpublished Work of Raytheon Electronic Systems

[11] M.J. Kuckelman, *Information Assurance Experiments Summary*, `iarm experiment review summary.ppt`, Unpublished Work of Raytheon Electronic Systems, January 2001

[12] R.L. Gotfried, IARM PI meeting 0301.ppt

[13] R.L. Gotfried, IARM PI 2Q01 Rvw.ppt